(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年4 月4 日 (04.04.2002)

PCT

(10) 国際公開番号
WO 02/27503 A1

(51) 国際特許分類[7]: G06F 13/00, H04L 12/66, G06F 15/00

(21) 国際出願番号: PCT/JP01/08449

(22) 国際出願日: 2001 年9 月27 日 (27.09.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-294568 2000 年9 月27 日 (27.09.2000) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 小林信司 (KOBAYASHI, Shinji) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 稲本義雄(INAMOTO, Yoshio); 〒160-0023 東京都新宿区西新宿7丁目11番18号 711ビルディング4階 Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

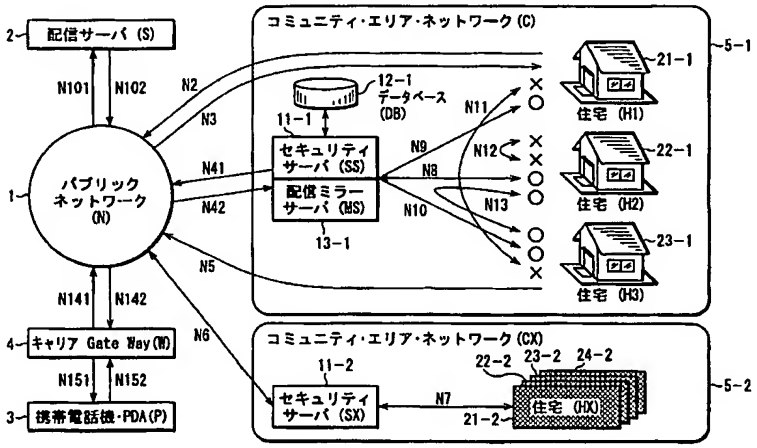
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: HOME NETWORK SYSTEM

(54) 発明の名称: ホームネットワークシステム



2...DISTRIBUTION SERVER (S)
1...PUBLIC NETWORK (N)
4...CARRIER GATEWAY (W)
3...PORTABLE TELEPHONE/PDA (P)
5-1...COMMUNITY AREA NETWORK (C)
12-1...DATABASE (DB)
11-1...SECURITY SERVER (SS)
13-1...DISTRIBUTION MIRROR SERVER (MS)
21-1...HOUSE (H1)
22-1...HOUSE (H2)
23-1...HOUSE (H3)
5-2...COMMUNITY AREA NETWORK (CX)
11-2...SECURITY SERVER (SX)
21-2...HOUSE (HX)

(57) Abstract: A home network in which security is ensured can be constructed even if the user has no special knowledge. An access from a house (21-1) in a community network (5-1) to an external public network (1) through a path (N2) needs no authentication by a security server (11-1). Apparatuses and machines in the house (21-1) reject any direct access from the public network (1) through a path (N3). When an access from a public network (1) through a path (N42) is made, the security server (11-1) performs authentication. If any correct result of the authentication is obtained, the access to the house (21-1) through a path (N9) is allowed.

WO 02/27503 A1

(57) 要約:

本発明は、ホームネットワークシステムに関する。専門的な知識を有さずとも、セキュリティが確保されたネットワークを構築できるようにする。コミュニティエリアネットワーク５－１内の住宅２１－１から外部のパブリックネットワーク１への経路Ｎ２を介してのアクセスは、セキュリティサーバ１１－１による認証処理が必要とされない。住宅２１－１の機器は、経路Ｎ３を介して、パブリックネットワーク１から直接行われるアクセスを拒否する。セキュリティサーバ１１－１は、パブリックネットワーク１から経路Ｎ４２を介してアクセスが行われたとき、認証処理を行い、正しい認証結果が得られたとき、住宅２１－１への経路Ｎ９を介してのアクセスを許容する。

明細書

ホームネットワークシステム

技術分野

本発明は、ホームネットワークシステムに関する。

背景技術

従来、一般の家庭からパブリックなネットワークに対し、常時接続される状況が少なかったため、ネットワークセキュリティに関する意識が少なかった。

従来、企業などでのネットワークセキュリティは、ファイアウォール(Firewall)などを用いて行われている。

Firewall を設置し、運用し、メンテナンスする場合、多くの専門知識を必要とし、一般の家庭で利用するのは、事実上不可能である。

一般の家庭でFirewallを設置せず、パブリックなネットワークへの常時接続を行った場合、家庭内ネットワークへの第３者の侵入が容易であるため、パスワード、クレジットＩＤ、電子商取引（ＥＣ）のＩＤなど、機密情報を盗まれる可能性がある。

一般の家庭で、ルータによるパブリックなネットワークへの常時接続を行った場合においても、フィルタリングはできるものの、個人認証などを別に行う必要がある場合は、認証システムを構築するための専門知識を必要とするため、一般の家庭で利用するのは、事実上不可能である。

さらに、携帯機器などにより、宅外から宅内のネットワーク機器にアクセスしようとする場合、認証システムがないため、セキュリティ上、防犯などセキュリティシステムの遠隔操作や宅内サーバからのデータダウンロードなどを行うことができない。

VoIP (Voice over IP) などを使ったネットワーク電話は、企業内での使用などを除き、通常、接続サーバに接続している相手のみを呼び出すようになっており、

一般の電話システムにおける電話番号での呼び出しのような、接続状態でないネットワーク電話を呼び出せるようにはなっていない。

現在、インターネットのようなパブリックなネットワークに常時接続する場合は、セキュリティを保つために、ルータなど接続装置によりフィルタリングや接続の制御を行うか、大掛かりなFirewallなどを設置するが、この場合、個別のネットワーク内の機器が隠蔽されるため、機器ごとにプッシュ（Push）型の配信を受けることは、ネットワークの知識を必要とし一般的に困難である。

発明の開示

本発明は、このような状況に鑑みてなされたものであり、専門的知識を有しない一般ユーザでも、簡単且つ確実にセキュリティを保持しつつ、外部と通信できるようにするものである。

本発明のホームネットワークシステムは、第１のネットワークと第２のネットワークとの間のアクセスの方向を検出する検出手段と、認証処理を行うのに必要な情報を記憶する記憶手段と、検出手段により第１のネットワークから第２のネットワークの方向へのアクセスが検出されたとき、記憶手段により記憶されている情報に基づいて認証処理を行う認証手段と、認証手段による認証結果に基づいて、第１のネットワークから第２のネットワークへのアクセスに基づく接続を制御する制御手段とを備えることを特徴とする。

前記認証手段は、検出手段により、第２のネットワークから第１のネットワークの方向へのアクセスが検出されたとき認証処理を行わないようにすることができる。

前記制御手段は、VPNを利用して接続を制御するようにすることができる。

前記第２のネットワークは、複数の居住空間における個々のネットワークにより構成されるようにすることができる。

前記複数の居住空間における個々のネットワークは、イーサネットまたはIEEE1394を含むようにすることができる。

前記認証手段は、ワイヤレスモバイル機器からの電話番号または機器IDを用いて認証処理を行うようにすることができる。

前記記憶手段は、第１のネットワークからの情報を第２のネットワークにプッシュ型配信するのに必要な情報をさらに記憶するようにすることができる。

前記プッシュ型配信される情報は、広告情報、行政情報、災害情報、または緊急情報を含むようにすることができる。

本発明の接続制御方法は、第１のネットワークと第２のネットワークとの間のアクセスの方向を検出し、認証処理を行うのに必要な情報を予め記憶し、第１のネットワークから第２のネットワークの方向へのアクセスが検出されたとき、記憶されている情報に基づいて認証処理を行い、認証結果に基づいて、第１のネットワークから第２のネットワークへのアクセスに基づく接続を制御することを特徴とする。

本発明のネットワークシステムは、家庭内の各種機器がネットワークにより相互接続され、また、物理層、プロトコルの異なるネットワーク間ではブリッジ（Bridge）などの利用により相互通信可能とする。

ルータなど通信データのルーティング、フィルタリングを行える機器により外部のネットワークと常時接続することが可能とするようにすることができる。

前記機器にコネクションコントロールを付加した機器により、外部のネットワークと常時接続することが可能とするようにすることができる。

前記機器により外部からのコネクションをコントロールし、信頼できる機器からの接続をVPNなどの技術を使い有効とする機能をもつようにすることができる。

本発明のコミュニティ・エリア・ネットワークは、複数の住宅（マンション、アパートなどを含む）または、住宅地が集まりネットワークを構成している。本発明のワイドエリア・コミュニティ・ネットワークは、複数のコミュニティ・エリア・ネットワークが集まり、ネットワークを構成している。

コンテンツ配信ミラーサーバ、広告配信サーバなど各種サービスを行うサーバを持ち、加えて、セキュリティを維持するセキュリティサーバを持つようにする

ことができる。

本発明のワイドエリア・コミュニティ・ネットワークは、セキュリティサーバは、パブリックネットワークからのコネクションに対しユーザ認証などを行いターゲットとなるユーザ宅内ネットワークのルータ､ゲートウェイなどにVPNなどの技術を使い接続する。

本発明のワイドエリア・コミュニティ・ネットワークは、携帯電話機器やPDAなどを使いパブリックネットワーク経由で接続する場合、電話番号などの識別符号や各種ＩＤをセキュリティサーバに送り、ユーザ認証に利用する。

本発明のワイドエリア・コミュニティ・ネットワークは、コミュニティ・エリア・ネットワークなどある範囲のネットワーク内において、セキュリティサーバは、トラフィック監視やルータなど接続装置の状況を監視し、記録を残し、問題発生時の警報や解析などをおこないセキュリティを確保する。

図面の簡単な説明

図１は、本発明を適用したシステムの構成を示すブロック図である。

図２は、本発明を適用した住宅内のネットワークの構成を示すブロック図である。

図３は、本発明を適用した住宅内のネットワークの構成を示すブロック図である。

図４は、セキュリティサーバの接続処理を説明するフローチャートである。

図５は、ルータのアクセス処理を説明するフローチャートである。

図６は、本発明を適用したワイドエリア・コミュニティ・ネットワークの構成を示すブロック図である。

図７は、通信の手順を説明する図である。

発明を実施するための最良の形態

図１は、本発明を適用したシステムの基本構成を示したものである。

図１の構成では、インターネットに代表されるパブリックネットワーク１とコンテンツなどを配信する配信サーバ２が経路Ｎ１０１,Ｎ１０２により接続され、パブリックネットワーク１と携帯電話機器、PDA（Personal Digital Assistants）などのワイヤレスモバイル機器３が、キャリアのゲートウェイ（Gate Way）４を経由して、経路Ｎ１４１，Ｎ１４２、Ｎ１５１，Ｎ１５２を通り接続される。

内部のネットワークとしてのコミュニティ・エリア・ネットワーク５－１は、住宅地やマンションなど集合住宅等、地理に依存した形態のネットワークで構成される場合や、ISP（Internet Service Provider）など地理的な依存が無いネットワーク形態で構成される場合がある。

コミュニティ・エリア・ネットワーク５－１には、セキュリティを維持するためのセキュリティサーバ１１－１、認証データや各住宅へのアクセスを行うためのプロファイルなどを保持するためのデータベース１２－１、コミュニティ・エリア・ネットワーク５－１内へ各種コンテンツを高品質に配信するための配信ミラーサーバ１３－１などが設置される。

配信ミラーサーバ１３－１は、配信サーバ２からコミュニティ・エリア・ネットワーク５内へ配信されるコンテンツをキャッシュするとともに、ミラーリングする。

配信ミラーサーバ１３－１は、コミュニティ・エリア・ネットワーク５－１までの回線状況によりコミュニティ・エリア・ネットワーク５－１内に必要が無い場合もある。

セキュリティサーバ１１－１は、外部のネットワークとしてのパブリックネットワーク１から経路Ｎ４２を介してのコミュニティ・エリア・ネットワーク５－１内へのアクセスに対し、アクセスしている機器のＩＤ(固有のＩＤや電話番号など)および暗証番号などをデータベース１２－１のデータと照合することで、アクセス可能であるか否かを認証する。

なお、図１の例では、コミュニティ・エリア・ネットワーク５－１と同様の構成のコミュニティ・エリア・ネットワーク５－２も、パブリックネットワーク１

に接続されている。

住宅内からパブリックネットワーク１を経由した配信サーバ２へのアクセスは、例えば、住宅２１－１からパブリックネットワーク１へ経路Ｎ２を経由し、さらにパブリックネットワーク１から経路Ｎ１０１を経由してコネクションを張ることで行われる。すなわち、コミュニティ・エリア・ネットワーク５－１から外部へのアクセスには、セキュリティサーバ１１は実質的に使用されない（使用されるとしても、認証処理等は実質的にスルーされる）。

この場合、例えばTCP/IP（Transmission Control Protocol/Internet Protocol）では、最初のパケットで、SYNビットがセットされ、ACKビットがリセットされている。

配信サーバ２からの返信は、配信サーバ２からパブリックネットワーク１へ経路Ｎ１０２を経由し、さらにパブリックネットワーク１から住宅２１－１へ経路Ｎ３を経由して行われる。

この場合、例えばTCP/IPでは、SYNビットがセットされ、ACKビットがセットされている。

以降、コネクションが確立している通信では、ACKビットがセットされている。

住宅２１－１から通信が開始されていない場合、まず、パブリックネットワーク１から住宅２１－１への経路Ｎ３で通信が開始され、その最初のパケットでSYNビットがセットされ、ACKビットがリセットされている。

住宅２１－１では、ルータ６１（後述する図２）により、ACKビットがリセットされている最初のパケットの転送方向（宛先アドレス）に基づいて、通信が住宅２１－１から開始されたものであるのか、またはパブリックネットワーク１から開始されたものであるのかを判定できる。

住宅２１－１では、ルータ６１により、パブリックネットワーク１からのアクセスであると判定された場合、コネクションを拒否することで、パブリックネットワーク１からの進入を拒否することができる。

正規のユーザが住宅２１－１の外部から、パブリックネットワーク１を経由し

て、住宅２１－１にアクセスする場合、例えば、携帯電話機器・PDAなどのワイヤレスモバイル機器３から経路Ｎ１５２を経由しキャリアGate Way４に対してキャリアによる通信が最初に行われ、回線が確保される。

次に、キャリアGate Way４でパブリックネットワーク１へ通信するためのプロトコル変換処理が行われ、経路Ｎ１４１を経由しパブリックネットワーク１に対して、さらに経路Ｎ４２を経由してセキュリティサーバ１１－１に対してコネクションが張られる。

セキュリティサーバ１１－１は上述したように、ワイヤレスモバイル機器３の機器ＩＤや暗証番号などに基づいて認証を行い、認証に成功した場合、データベース１２－１のプロファイルにしたがって、接続先、例えば住宅２１－１に、経路Ｎ９を介して、VPN（Virtual Private Network）などの技術を使い接続をする。

住宅２１－１（ルータ６１）は、信頼できるセキュリティサーバ１１－１からVPNなどの技術を使い接続される場合のみ接続を許可し、この経路Ｎ９でのコネクションを確立する。

上記により外部からの住宅２１－１に対するコネクションが可能となる。

プッシュ型配信は、配信サーバ２から経路Ｎ１０２、パブリックネットワーク１、経路Ｎ４２を経由しセキュリティサーバ１１－１に送られる。

セキュリティサーバ１１－１は、データベース１２－１に登録されている情報から配信すべきものかを判断し、配信すべきものであれば、配信情報、または、データベース１２－１の登録情報を基に、住宅内の機器にVPNなどの技術を使い配信する。これにより、地域密着型の広告や、行政情報、緊急情報、災害情報などを、プッシュ型配信することができる。このため、データベース１２－１には、このようなプッシュ型配信を許容するか否かを判断するために必要な情報が予め登録されている。

コミュニティ・エリア・ネットワーク５－１内においては、基本的に、例えば、住宅２１－１と住宅２２－１間で、通信のための接続が行われてはならない。

そのため、各住宅（ルータ６１）は、パブリックネットワーク１との通信と同

様に、外部からの通信については、経路Ｎ１２（住宅２１と住宅２２の間の通信）、経路Ｎ１１（住宅２１－１と住宅２３－１との間の通信）のような、同一のコミュニティ・エリア・ネットワーク５－１内の住宅からの接続をも拒否する必要がある。

ただし、例えば、住宅２２－１と住宅２３－１は、お互いに緊急時連絡先の指定をしてある場合、住宅２２－１から緊急情報をセキュリティサーバ１１－１に発信すると、セキュリティサーバ１１－１では、データベース１２－１に登録されている情報を基に、住宅２３－１へVPNなどの技術を使い接続し、緊急情報を指定機器にプッシュ型配信する。

これにより、コミュニティ・エリア・ネットワーク５－１内の緊急時相互援助が可能となる。

図２は、図１のコミュニティ・エリア・ネットワーク５－１，５－２を構成する住宅内のネットワークの基本的な構成を示したものである。

住宅内のネットワークとしての、例えば経路Ｎ２１と、パブリックネットワーク１、およびセキュリティサーバ１１－１との接続は、ルータ６１を介して、経路Ｎ２０により行われる。

ルータ６１は、アドレス、ポート、入出力などの条件による基本的なフィルタ機能を備え、上述したように説明したフィルタ機能、信頼できる特定の機器（図１の例の場合、セキュリティサーバ１１－１）からの接続要求のみを受け付ける機能、VPNなどのトンネリング機能を実装する。

ルータ６１は、その他、アドレス・ポート変換機能、ストリーミングに対応する場合は、QoS（Quality of Service）の機能、必要がある場合はHUB機能、DNS（Domain Name System）、DHCP（Dynamic Host Configuration Protocol）などのデバイスディスカバリー機能を有する。

経路Ｎ２１は、住宅内のバックボーンとなる高速なネットワークであり、例えばイーサネット（Ethernet）（商標）などが用いられる。

この高速なネットワークとしての経路Ｎ２１には、VoIP機能を備え、ネットワ

ークを経由しコミュニケーションができる電話機（TEL）６２、ストリームやデータの記録、再生、再配信などを行うサーバ（Server）６３、テープメディアやディスクメディアなどにストリームやデータの記録、再生、再配信などを行うビデオカセットレコーダー（VCR）６４、ストリーミングオーディオやネットワークラジオ放送を受信したり、再配信などを行うオーディオ機器（Audio）６５、ネットワーク対戦ゲームなどに対応したゲーム機器（Game）６６、映像コンテンツやデジタル放送、ストリーミング放送などを受信し映像を表示するデジタルテレビジョン受像機（DTV）６７、パーソナルコンピュータ（ＰＣ）６８などが接続される。

経路Ｎ２２は、住宅内でも低速なネットワークであり、防犯、火災などのセキュリティセンサ７１、給湯、照明、給電などの住宅設備機器７２、ドアロックなどアクチュエータ機器の制御を行うアクチュエータコントローラ７３などが接続される。

これらの機器は、高速なネットワークとしての経路Ｎ２１とブリッジ（Bridge）７０で接続され、プロトコル変換、物理メディア変換などは、ブリッジ７０が行う。

図３は、図１のコミュニティ・エリア・ネットワーク５－１，５－２を構成する住宅内のネットワークの他の構成例を表し、この例では、図２のネットワークに、さらに、例えば、IEEE1394などの、所定の分野に特化したネットワークが接続されている。

経路Ｎ３３は、例えば、IEEE1394により構成されるＡＶシステムのネットワークで、経路Ｎ３１は、経路Ｎ２１と同様の宅内バックボーンであり、例えばイーサネットである。

経路Ｎ３３は、ブリッジ９１により経路Ｎ３１に接続され、ブリッジ９１は経路３３と経路Ｎ３１との間の、プロトコル変換、物理メディア変換などを行う。

このようなブリッジを介して各種のネットワークを接続する構成を採ることにより、宅内のネットワークは、柔軟に最新の技術に対応することが可能である。

セキュリティサーバ１１－１における接続処理をまとめると、図４のフローチ

ャートに示されるようになる。すなわち、セキュリティサーバ１１－１は、ステップＳ１１において、アクセスの方向を検出する。すなわち、コミュニティ・エリア･ネットワーク５－１からパブリックネットワーク１の方向へのアクセス(内部から外部へのアクセス）であるのか、または、逆に、パブリックネットワーク１からコミュニティ・エリア・ネットワーク５－１へのアクセス（外部から内部へのアクセス）であるのかが検出される。ステップＳ１２において、セキュリティサーバ１１－１は、ステップＳ１１における検出結果が、外部から内部へのアクセスであるか否かを判定する。外部から内部へのアクセスである場合には、ステップＳ１３に進み、セキュリティサーバ１１－１は、上述したようにして認証処理を行う。この認証処理には、上述したように、例えば、ワイヤレスモバイル機器３から取得した電話番号や機器ＩＤなどが用いられるとともに、データベース１２－１に登録されている情報が利用される。

ステップＳ１４において、セキュリティサーバ１１－１は、認証結果がＯＫであったか否かを判定し、認証結果がＯＫである場合には、ステップＳ１５に進み、接続処理を実行する。すなわち、セキュリティサーバ１１－１は、パブリックネットワーク１を介して、アクセスしてきた外部の機器を、住宅２１－１の機器に接続するための処理を実行する。この処理は、経路Ｎ４２、Ｎ９を経由した処理に対応する。

これに対して、ステップＳ１２において、認証ＯＫの結果が得られなかった場合には、ステップＳ１６に進み、セキュリティサーバ１１－１は、接続拒否の処理を実行する。

ステップＳ１２において、外部から内部へのアクセスではないと判定された場合（内部から外部へのアクセスであると判定された場合）、セキュリティサーバ１１－１は、ステップＳ１３の処理をスキップし、ステップＳ１５に進み、直ちに接続処理を実行する。この処理は、経路Ｎ２を介しての処理に対応する。

また、ルータ６１のアクセス処理をまとめると、図５のフローチャートに示されるようになる。

すなわち、ステップＳ３１において、ルータ６１は、アクセスするのか否かを判定する。アクセスを受けるのではなく、アクセスする場合は、ステップＳ３２に進み、ルータ６１は、外部へのアクセスであるのか否かを判定する。外部へのアクセスである場合には、ステップＳ３３に進み、ルータ６１は、アクセスを実行する。この処理は、例えば経路Ｎ２を介してのアクセスに対応する。

ステップＳ３２において、外部へのアクセスではないと判定された場合（内部へのアクセスであると判定された場合）、ステップＳ３４に進み、ルータ６１は、アクセスを拒否する処理を実行する。この処理は、例えば、経路Ｎ１１によるアクセスに対応する。

ステップＳ３１において、アクセスするのではないと判定された場合（アクセスを受けると判定された場合）、ステップＳ３５に進み、ルータ６１は、セキュリティサーバ１１－１からのアクセスであるか否かを判定する。セキュリティサーバ１１－１からのアクセスである場合には、ステップＳ３６に進み、ルータ６１は、アクセスを受ける処理を実行する。このアクセスは、例えば、経路Ｎ４２と経路Ｎ９を介してのアクセスに対応する。

これに対してステップＳ３５において、セキュリティサーバ１１－１からのアクセスではないと判定された場合、ステップＳ３７に進み、ルータ６１は、アクセスを拒否する処理を実行する。例えば、このアクセスは、経路Ｎ３を介してのアクセスに対応する。

図６は、内部のネットワークが、より広いネットワークであるワイドエリア・コミュニティ・ネットワーク１１１により構成される場合の例を表している。ワイドエリア・コミュニティ・ネットワーク１１１は、複数のコミュニティ・エリア・ネットワーク５－１乃至５－ｎにより構成され、各コミュニティ・エリア・ネットワーク５－１乃至５－ｎは、データベース１２、セキュリティサーバ１１、配信ミラーサーバ１３を共有している。

図７は、VoIPなどネットワークを経由し利用できる電話機を実用的に利用するため、電話番号変換ルートサーバ１２１を構成に採りこんだ例である。

VoIPは通常ＩＰアドレスを指定することで、呼び出しを行い通信路を確定するが、ＩＰアドレスは覚えにくく、一般的ではない上に、ＩＰアドレス自体が接続形態により変化するため、ITU-T E.164などが利用される。

図７において、住宅２１－１のVoIP電話機６６から、住宅２３－１に電話番号を用いてCallした場合、経路Ｎ５２、パブリックネットワーク１、経路Ｎ５６１を介して電話番号変換ルートサーバ１２１に対しセットアップを行うための通信が行われる。

電話番号変換ルートサーバ１２１は、データベース１２２に登録されている情報に基づいて、電話番号をＩＰアドレスに変換し、経路Ｎ５６２、パブリックネットワーク１、経路Ｎ５５２、セキュリティサーバ１１－１、経路Ｎ５１０を介し、住宅２３－１のVoIP電話機に接続する。

この場合、セキュリティサーバ１１－１は、住宅２３－１内のVoIP電話機に関する情報をデータベース１２－１から引き出し、また、セキュリティサーバ１１－１は、住宅２３－１のVoIP電話機のプロキシ（Proxy）として返答を行う。

ＩＰアドレスが変化する環境では、電話番号変換ルートサーバ１２１にVoIP電話機やプロキシから、電話番号とそれに対応するＩＰアドレスの登録を、ダイナミックに更新する手段を備える必要がある。

このように、内部のネットワークとしてのコミュニティ・エリア・ネットワーク５やワイドエリア・コミュニティ・ネットワーク１１１ごとに、セキュリティサーバ１１、データベース１２、配信ミラー１３を設けることで、各住宅では専門的知識を必要とせず、セキュリティを確保しつつ、外部のネットワークと常に接続することが可能となる。

これにより、本発明は、次のようなサービスを提供する場合に適用可能である。

（１）セキュリティ系サービス

情報：各家庭にFirewallを設置する必要のない、ネットワークセキュリティサービス

防犯：防犯的な異常を検知した場合、指定連絡先および、コミュニティ内

の交番、警察署等に自動通知などを行うサービス

安全： 緊急時(ガス漏れ、火事、急病など)に近くの指定した家に通報する地域相互援助サービス

（２）宅外からのアクセスサービス

宅外からの携帯電話機器、PDAなどによる自宅へのセキュアな接続サービス

（３）VoIP電話サービス

電話番号－ＩＰアドレス変換とセキュリティサーバのプロキシにより、電話番号での呼び出しを可能としたことで、VoIPをより利用しやすくしたネットワーク型電話サービス

（４）広告配信サービス

コミュニティネットワーク内の配信ミラーサーバを利用した地域密着型のプッシュ型広告配信サービス

（５）行政などインフォメーションサービス

行政情報の配信、緊急警報、注意報など災害情報のプッシュ型配信サービス

産業上の利用可能性

一般家庭からインターネットなどのパブリックなネットワークに対し常時接続されるような場合にも、ユーザはセキュリティを意識せず、かつ、専門的な知識が無くても、セキュリティの確保されたネットワーク環境を利用することが可能となる。

宅外からの携帯電話機器やPDAなどを用いた、宅内のネットワークへの、セキュリティを確保したアクセス環境を提供することで、宅内機器の監視、操作、やり取りなどが可能となり、防犯、安全、急病などを意識した通信の対応、各種データのシームレスな利用などが行える。

コミュニティ・エリア・ネットワーク等、ネットワークの有効範囲を確定することで、状況、状態の把握が容易になり、システムの安定な動作とセキュリティ

の確保が可能となる。

キュリティサーバなど特定の経路からのコネクションのみを許可することで、セキュリティを保ち、ルータなど接続機器の遠隔設定、保守などを行うことが可能となる。

上述した場合と同様に、セキュリティを保ち、宅内のネットワーク機器などの遠隔保守なども可能となる。

請求の範囲

1． 外部の第１のネットワークに接続される内部の第２のネットワークを含むホームネットワークシステムにおいて、

前記第１のネットワークと前記第２のネットワークとの間のアクセスの方向を検出する検出手段と、

認証処理を行うのに必要な情報を記憶する記憶手段と、

前記検出手段により前記第１のネットワークから前記第２のネットワークの方向へのアクセスが検出されたとき、前記記憶手段により記憶されている情報に基づいて認証処理を行う認証手段と、

前記認証手段による認証結果に基づいて、前記第１のネットワークから前記第２のネットワークへのアクセスに基づく接続を制御する制御手段と

を備えることを特徴とするホームネットワークシステム。

2． 前記認証手段は、前記検出手段により、前記第２のネットワークから前記第１のネットワークの方向へのアクセスが検出されたとき認証処理を行わない

ことを特徴とする請求項１に記載のホームネットワークシステム。

3． 前記制御手段は、VPNを利用して接続を制御する

ことを特徴とする請求項１に記載のホームネットワークシステム。

4． 前記第２のネットワークは、複数の居住空間における個々のネットワークにより構成される

ことを特徴とする請求項１に記載のホームネットワークシステム。

5． 前記複数の居住空間における個々のネットワークは、イーサネットまたはIEEE1394を含む

ことを特徴とする請求項４に記載のホームネットワークシステム。

6． 前記認証手段は、ワイヤレスモバイル機器からの電話番号または機器IDを用いて前記認証処理を行う

ことを特徴とする請求項１に記載のホームネットワークシステム。

7． 前記記憶手段は、前記第１のネットワークからの情報を前記第２のネット

ワークにプッシュ型配信するのに必要な情報をさらに記憶する

ことを特徴とする請求項１に記載のホームネットワークシステム。

８．　前記プッシュ型配信される情報は、広告情報、行政情報、災害情報、または緊急情報を含む

ことを特徴とする請求項７に記載のホームネットワークシステム。

９．　外部の第１のネットワークに接続される内部の第２のネットワークを含むホームネットワークシステムの接続制御方法において、

前記第１のネットワークと前記第２のネットワークとの間のアクセスの方向を検出し、

認証処理を行うのに必要な情報を予め記憶し、

前記第１のネットワークから前記第２のネットワークの方向へのアクセスが検出されたとき、記憶されている情報に基づいて認証処理を行い、

認証結果に基づいて、前記第１のネットワークから前記第２のネットワークへのアクセスに基づく接続を制御する

ことを特徴とする接続制御方法。

図 1

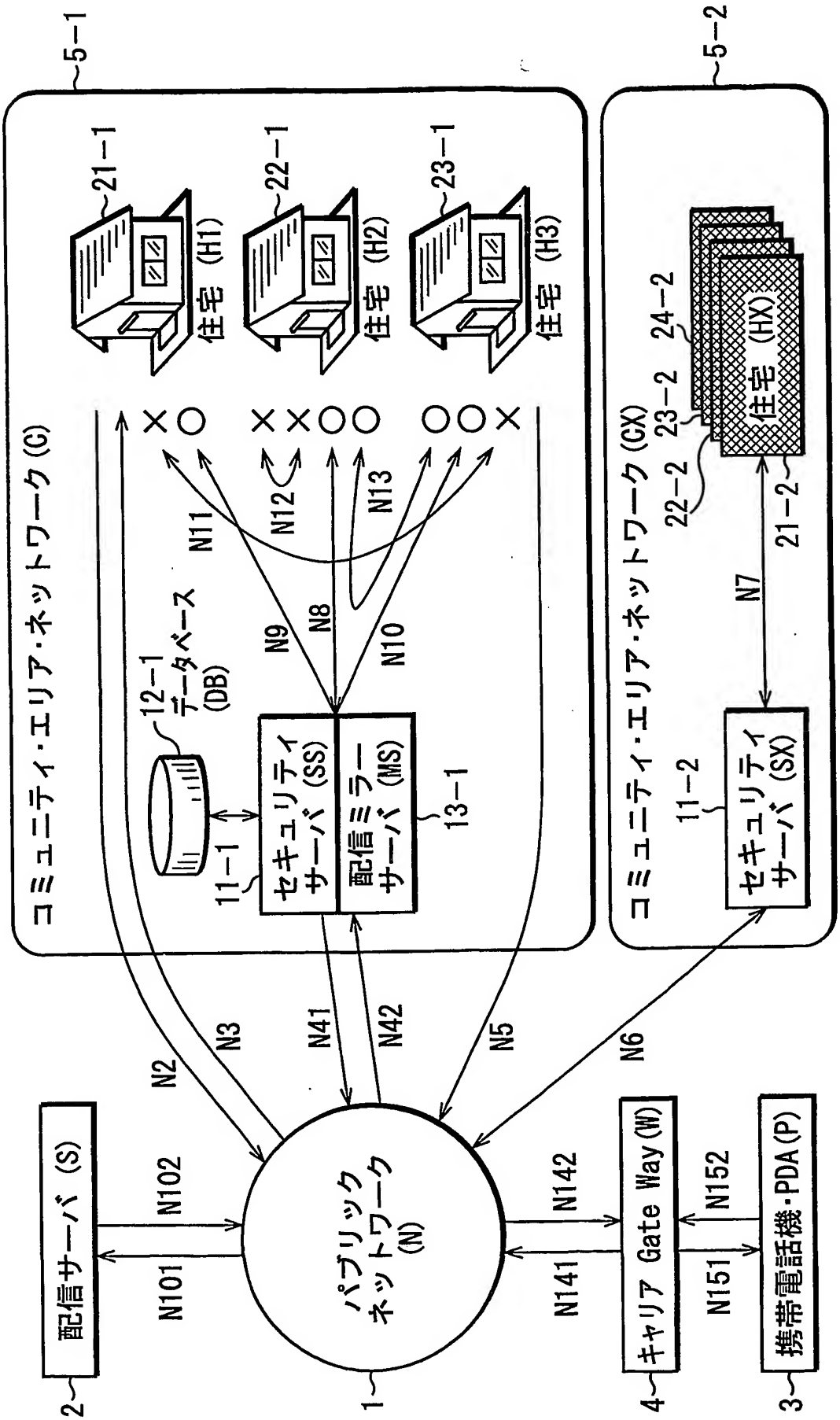

5-1
5-2
21-1
住宅 (H1)
22-1
住宅 (H2)
23-1
住宅 (H3)
24-2
住宅 (HX)
23-2
22-2
21-2
N11
N12
N13
N9
N8
N10
N7
12-1
データベース
(DB)
11-1
セキュリティ
サーバ (SS)
配信ミラー
サーバ (MS)
13-1
11-2
セキュリティ
サーバ (SX)
コミュニティ・エリア・ネットワーク (C)
コミュニティ・エリア・ネットワーク (CX)
N2
N3
N41
N42
N5
N6
配信サーバ (S)
N102
N101
パブリック
ネットワーク
(N)
N142
N141
キャリア Gate Way (W)
N152
N151
携帯電話機・PDA (P)
2
1
4
3

図2

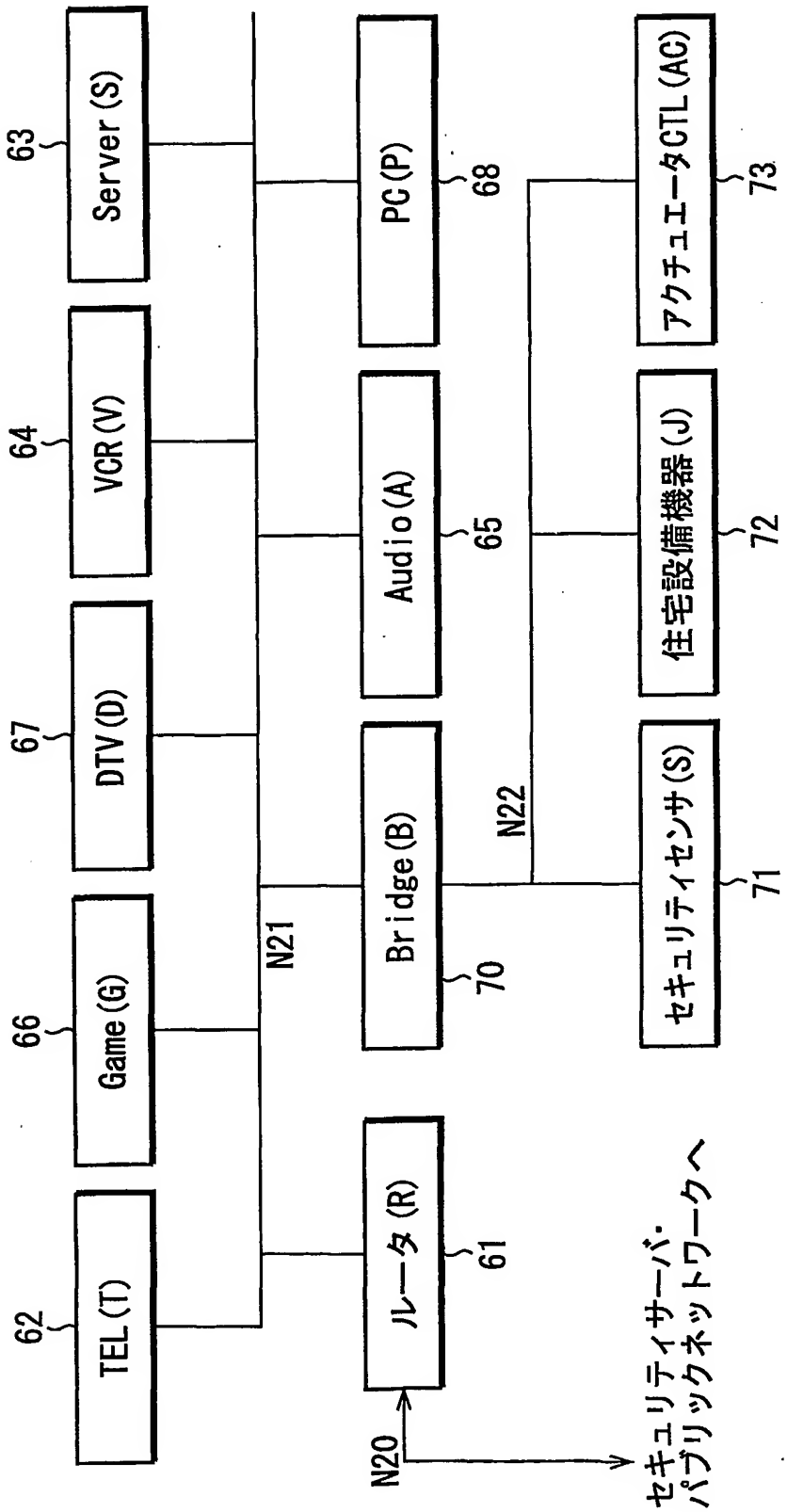

Server (S)
63
VCR (V)
64
DTV (D)
67
Game (G)
66
TEL (T)
62
PC (P)
68
Audio (A)
65
Bridge (B)
70
ルータ (R)
61
N21
N22
N20
アクチュエータCTL (AC)
73
住宅設備機器 (J)
72
セキュリティセンサ (S)
71
セキュリティサーバ・
パブリックネットワークへ

図3

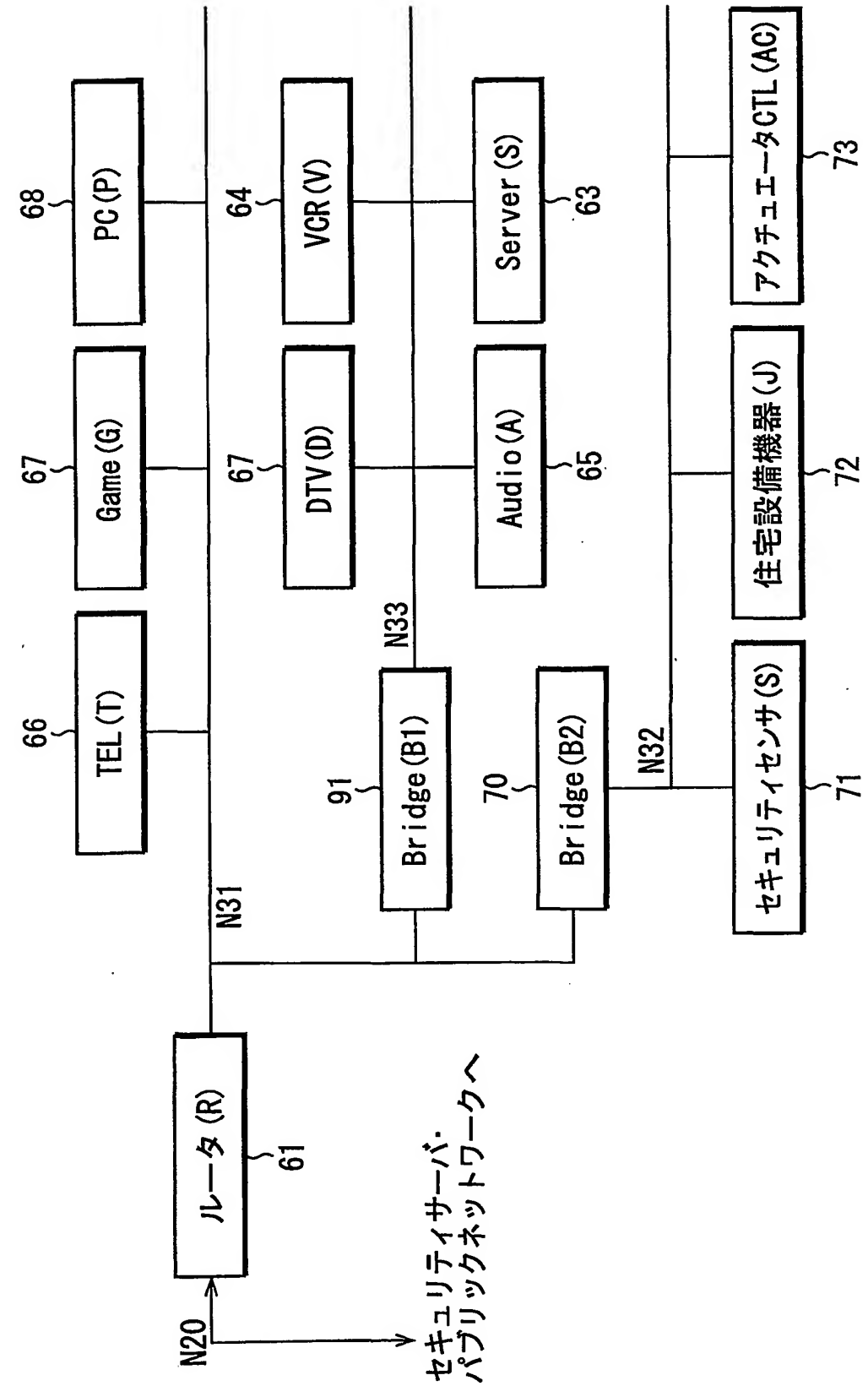

ルータ (R)
61
N20
セキュリティサーバ・
パブリックネットワークへ
N31
N32
N33
PC (P)
68
Game (G)
67
TEL (T)
66
VCR (V)
64
DTV (D)
67
Bridge (B1)
91
Server (S)
63
Audio (A)
65
Bridge (B2)
70
アクチュエータCTL (AC)
73
住宅設備機器 (J)
72
セキュリティセンサ (S)
71

図４

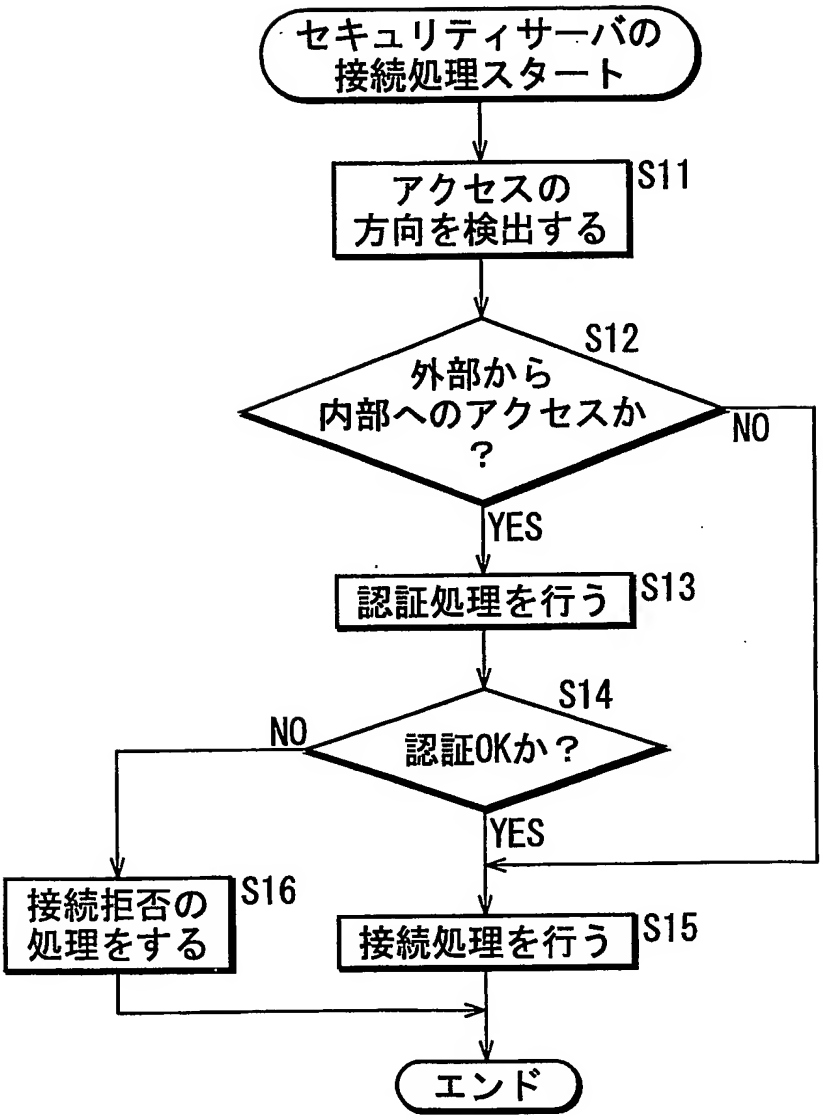

セキュリティサーバの
接続処理スタート
アクセスの
方向を検出する
S11
外部から
内部へのアクセスか
？
S12
NO
YES
認証処理を行う
S13
認証OKか？
S14
NO
YES
接続拒否の
処理をする
S16
接続処理を行う
S15
エンド

図５

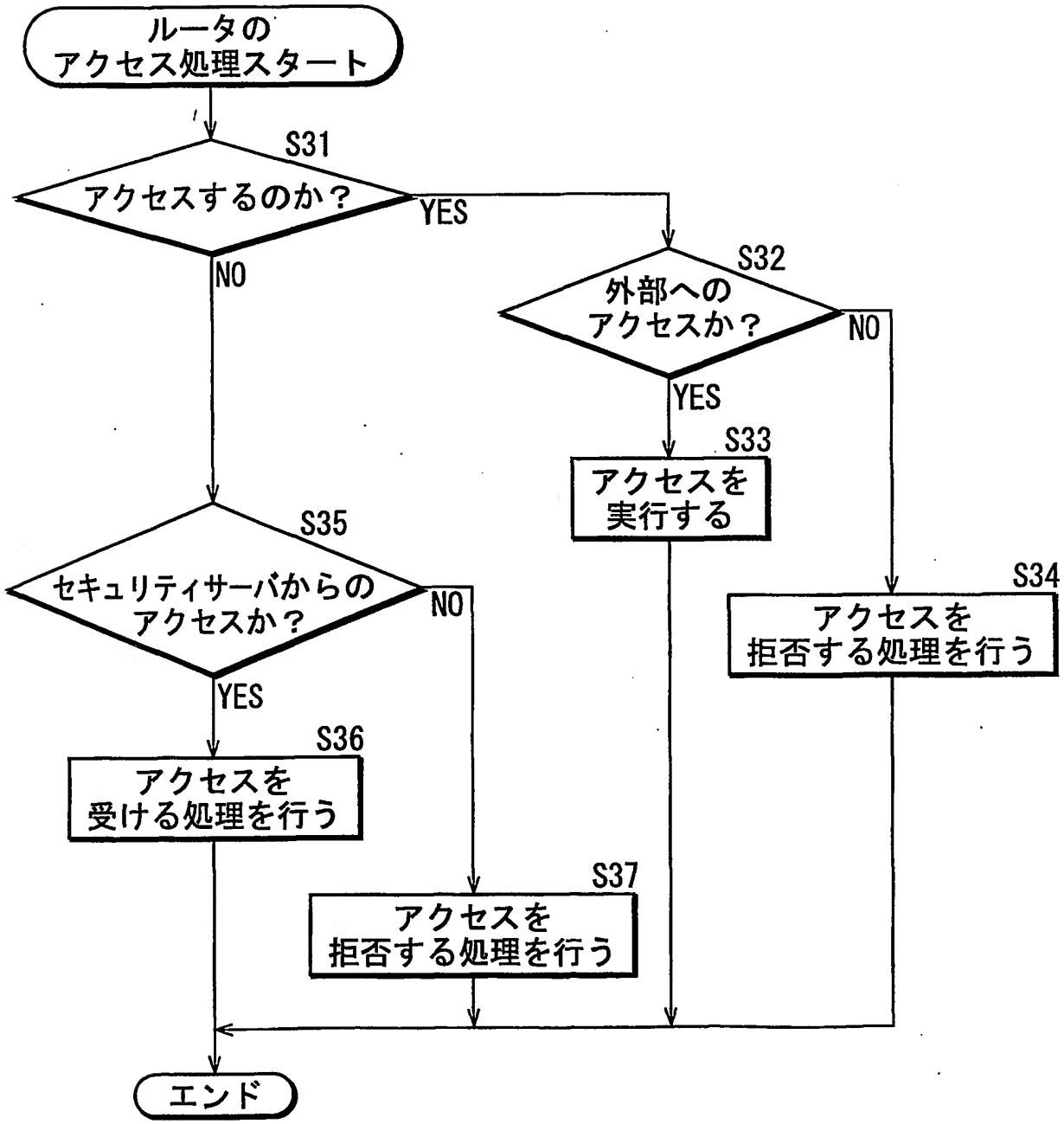

ルータの
アクセス処理スタート
S31
アクセスするのか？
YES
NO
S32
外部への
アクセスか？
NO
YES
S33
アクセスを
実行する
S34
アクセスを
拒否する処理を行う
S35
セキュリティサーバからの
アクセスか？
NO
YES
S36
アクセスを
受ける処理を行う
S37
アクセスを
拒否する処理を行う
エンド

図6

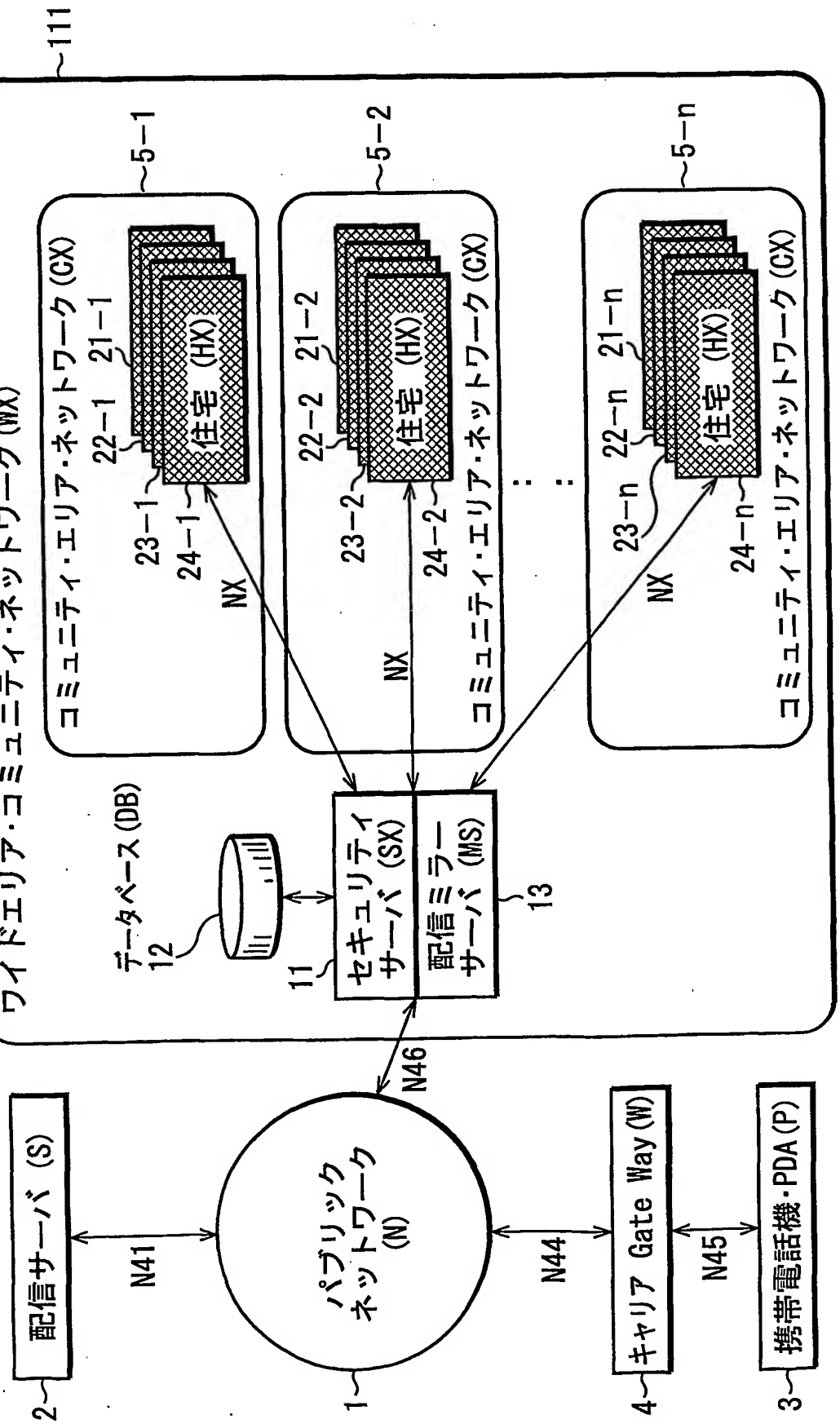
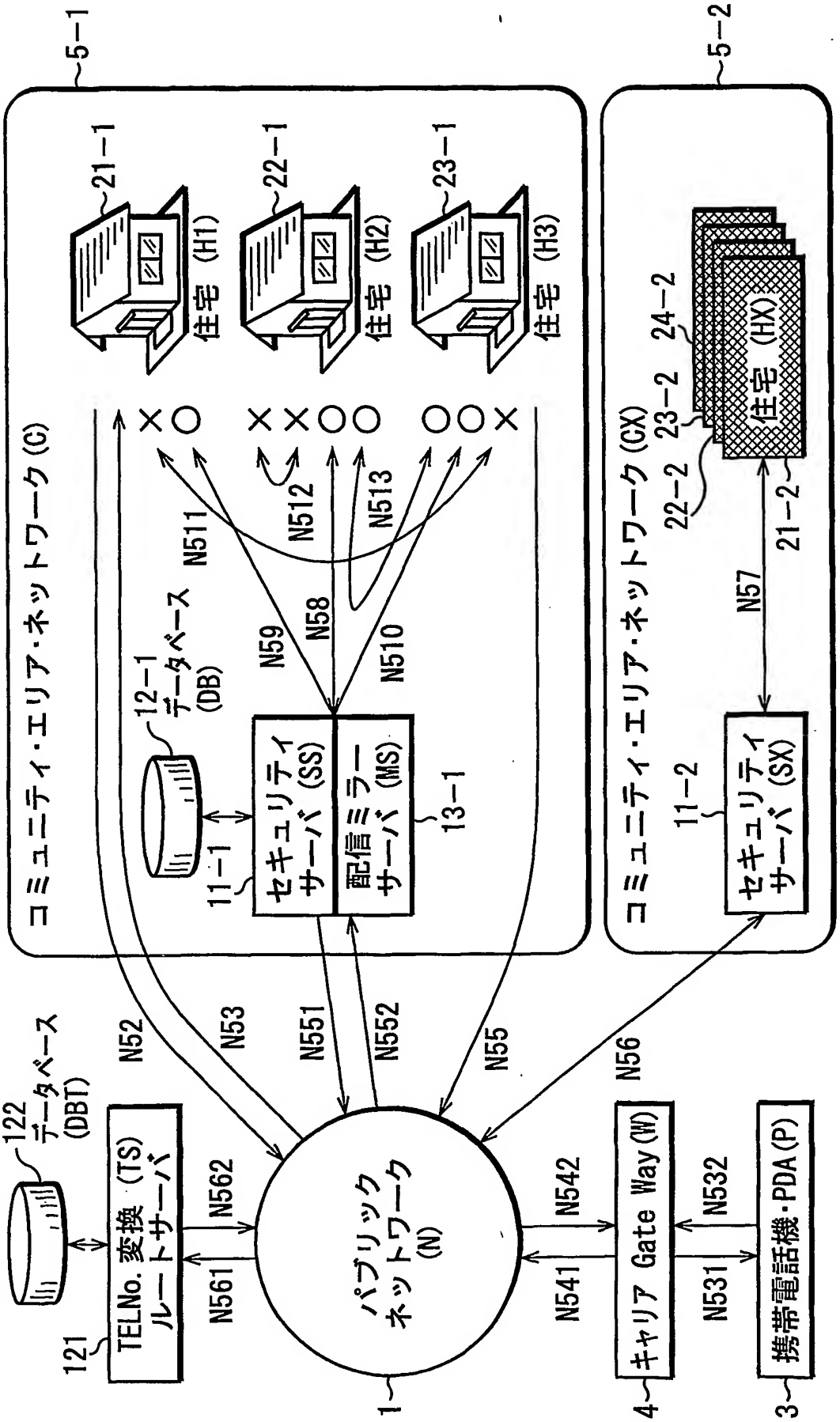

111
ワイドエリア・コミュニティ・ネットワーク (WX)
5-1
コミュニティ・エリア・ネットワーク (CX)
21-1
22-1
住宅 (HX)
23-1
24-1
NX
5-2
21-2
22-2
住宅 (HX)
23-2
24-2
NX
コミュニティ・エリア・ネットワーク (CX)
5-n
21-n
22-n
住宅 (HX)
23-n
24-n
NX
コミュニティ・エリア・ネットワーク (CX)
データベース (DB)
12
11
セキュリティサーバ (SX)
配信ミラーサーバ (MS)
13
N46
配信サーバ (S)
2
N41
パブリックネットワーク (N)
1
N44
キャリア Gate Way (W)
4
N45
携帯電話機・PDA (P)
3

図7


5-1
5-2
21-1
住宅 (H1)
22-1
住宅 (H2)
23-1
住宅 (H3)
24-2
住宅 (HX)
23-2
22-2
21-2
コミュニティ・エリア・ネットワーク (C)
コミュニティ・エリア・ネットワーク (CX)
N511
N512
N513
N59
N58
N510
N57
12-1
データベース
(DB)
11-1
セキュリティ
サーバ (SS)
配信ミラー
サーバ (MS)
13-1
11-2
セキュリティ
サーバ (SX)
N52
N53
N551
N552
N55
N56
122
データベース
(DBT)
TELNo. 変換
ルートサーバ (TS)
121
N562
N561
パブリック
ネットワーク
(N)
1
N542
N541
キャリア Gate Way (W)
4
N532
N531
携帯電話機・PDA (P)
3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/08449

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F 13/00, H04L 12/66, G06F 15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F 13/00, H04L 12/66, G06F 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-88406 A (Toshiba Corporation), 30 March, 1999 (30.03.99), Par. Nos. [0002]-[0011], [0024], [0101] to [0107], [0223]; Fig. 1 (Family: none)	1-9
Y	Ascii NT, Vol. 4, No. 2, February, 1999 KAGA "Policy Base no Tougou-teki na Security Taisaku wo Kanou ni suru Fire Wall-1", page 180, especially, right column, lines 10-16	1-9
Y	JP 11-175477 A (Casio Computer Co., Ltd.), 02 July, 1999 (02.07.99), Full text; Figs. 1 to 8 & EP 862104 A2 & CN 1193862 A & US 6108790 A1	6
Y	JP 11-239169 A (Sumitomo Electric Industries, Ltd.), 31 August, 1999 (31.08.99), Full text; Figs. 1 to 10 (Family: none)	7,8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 December, 2001 (04.12.01)	11 December, 2001 (11.12.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer

国際調査報告	国際出願番号 PCT／JP01／08449

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F 13／00, H04L 12／66, G06F 15／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F 13／00, H04L 12／66, G06F 15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2001年
日本国登録実用新案公報　1994－2001年
日本国実用新案登録公報　1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示.	関連する請求の範囲の番号
Y	JP 11－88406 A（株式会社東芝） 30. 3月. 1999（30. 03. 99） 段落番号【0002】～【0011】，【0024】 【0101】～【0107】，【0223】，第1図 （ファミリーなし）	1-9
Y	アスキーNT，第4巻，第2号，2月. 1999 加賀「ポリシーベースの統合的なセキュリティ対策を可能にするファイアウォール FireWall－1」 p. 180　特に右欄10-16行目参照	1-9

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
04. 12. 01	11.12.01

国際調査機関の名称及びあて先
日本国特許庁（ISA／JP）
郵便番号100－8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）
竹井　文雄　印
5R　3051

電話番号　03－3581－1101　内線　3565

国際調査報告

国際出願番号 PCT／JP01／08449

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 11－175477 A（カシオ計算機株式会社） 2. 7月. 1999（02. 07. 99） 全文，第1-8図 & EP 862104 A2 & CN 1193862 A & US 6108790 A1	6
Y	JP 11－239169 A（住友電気工業株式会社） 31. 8月. 1999（31. 08. 99） 全文，第1-10図（ファミリーなし）	7,8